

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 10.

Write $N(q)$ for the number of primes p with $p \leq q$. Suppose $n = p_1 \cdots p_k$ is the factorization of n into primes, written in non-decreasing order. Suppose that we have a table of primes less than or equal to \sqrt{n} . Then the number of operations needed to factor n is

$$k + N(m), \quad \text{where} \quad m = \max\{\sqrt{p_k}, p_{k-1}\}.$$

Now $k < \log_2 n$ and as we mentioned in Lecture 1, $N(m) \sim m/\log m$. The worst case is when n is prime and then $m = \sqrt{n}$ and the number of operations is order $\sqrt{n}/\log \sqrt{n}$.

The storage needed for a number of size n is $t = \log_2 n = c \log n$. The factorization time is at worst $e^{ct}/t > e^{c't}$ where $c' > 0$. This is exponential time. It is possible to check whether a number is prime in time t^{12} - polynomial time. At present we cannot factor in polynomial time, and it may be impossible to.

Irrationals $\sqrt{2}$ is irrational.

Proof. Suppose $2 = (a/b)^2$. We can suppose $(a, b) = 1$. Then $a^2 = 2b^2$ so $2|a^2$ so $2|a$ so $a = 2c$ and $4c^2 = 2b^2$ so $2c^2 = b^2$ so $2|b$ which is a contradiction since $(a, b) = 1$.

The same argument shows that $\sqrt{p_1 \cdots p_k}$ is irrational if p_1, \dots, p_k are distinct primes.

Modular Arithmetic We covered 3.1.1, 3.1.7, 3.1.13, 3.1.14, 3.1.15, we computed that 2^{100} has remainder 1 when divided by 11, and we did the exercise after 3.1.8, and covered 3.1.12.

Homework solution: $p, p + 2$ and $p + 4$ cannot all be prime, unless $p = 3$. To see this,

$$\begin{aligned} p \equiv 0 \pmod{3} &\Rightarrow p + 2 \equiv 2 \pmod{3}, & p + 4 \equiv 1 \pmod{3}, \\ p \equiv 1 \pmod{3} &\Rightarrow p + 2 \equiv 0 \pmod{3}, & p + 4 \equiv 2 \pmod{3}, \\ p \equiv 2 \pmod{3} &\Rightarrow p + 2 \equiv 1 \pmod{3}, & p + 4 \equiv 0 \pmod{3}, \end{aligned}$$

We see that 3 divides one of $p, p + 2$ or $p + 4$. If these are all prime, this implies $p = 3, p + 2 = 3$ or $p + 4 = 3$, but the latter two cases p is not prime, so the only case left is $p = 3$.